Monitoreo de riesgos de activos de información en la Universidad Nacional de Río Negro

Peña, Ricardo Luis; Lugani, Carlos Fabián

LIA - Laboratorio de Informática Aplicada – Sede Atlántica – Universidad Nacional de Río Negro
{rlpena; clugani} @unrn.edu.ar

Resumen. La seguridad de la información contempla el análisis de los riesgos existentes en los activos informáticos de una organización y el diseño de procesos para su tratamiento. No obstante, es en la implementación y monitoreo de la gestión de los riesgos donde se verifica realmente la efectividad del proceso y su valor para la organización. En este sentido en el presente trabajo se desarrollan herramientas para este fin entre las que se mencionan: un modelo de Estructura de Desglose de Riesgos, Matriz de probabilidad e impacto y una Guía de actividades para el Monitoreo de riesgos. De esta manera, se continúa completando el esquema para la Gestión de Riesgos definido por Lugani y Peña (2018) en el trabajo Desarrollo de un esquema de Gestión de Riesgos Informáticos en la Universidad Nacional de Río Negro.

Palabras clave: gestión de riesgos informáticos, matriz de probabilidad e impacto, monitoreo de riesgos

1 Introducción

El presente trabajo tiene como finalidad continuar con el desarrollo de un proceso de gestión de riesgos informáticos, incluyendo las actividades de monitoreo y evaluación. Este proceso complementa el esquema elaborado anteriormente por Lugani y Peña (2018) Desarrollo de un esquema de Gestión de Riesgos Informáticos en la Universidad Nacional de Río Negro. Implementar la gestión de riesgos a partir del mencionado esquema requiere la disponibilidad y disposición de herramientas destinadas a tal fin. Se desarrolló una estructura jerárquica para la clasificación de riesgos en activos informáticos, con el objeto de brindar una visión global de las amenazas, teniendo también en cuenta aquellas no técnicas. Luego se definieron valores para el análisis

cuantitativo de los riesgos en función de su probabilidad e impacto, resultando en una matriz de riesgos según su criticidad. Por último, se propuso un esquema de actividades y entregables para desarrollar el monitoreo y evaluación del proceso. De esta manera, se completó la definición del esquema basado en cuatro fases: análisis de riesgos, diseño del tratamiento de riesgos, implementación de la gestión de riesgos y monitoreo. En la Figura 1.1 se observa el mencionado esquema.

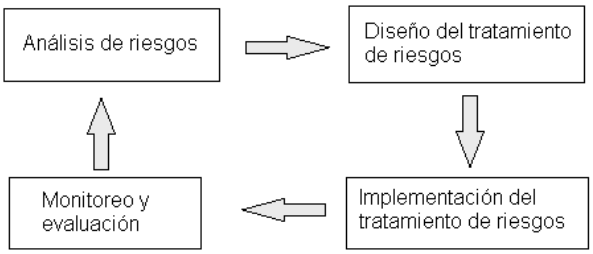

Figura 1.1. Esquema de cuatro fases para la gestión de riesgos en la UNRN.

2. Implementación de la gestión de riesgos

En el esquema definido por Lugani y Peña (2018) se plantean actividades para identificar los riesgos. No obstante, es necesario definir claramente herramientas que faciliten la clasificación de los riesgos identificados. Para esto, es necesario estandarizar la criticidad de los riesgos a través de una tabla con valores para la probabilidad de ocurrencia e impacto, y el consecuente armado de la matriz de control de riesgos. Otra utilidad complementaria al esquema es el establecimiento de una estructura jerárquica que permita clasificar los riesgos según distintas categorías y niveles. Ambas herramientas favorecen a una mejor implementación de la gestión de riesgos.

2.1. Relevamiento jerárquico de riesgos

Para facilitar y optimizar la identificación de los riesgos, es necesario contar con algún esquema o modelo que permita analizar estas eventualidades desde una visión global hasta una más específica. Una herramienta efectiva es la Estructura de Desglose del Riesgo (Risk Breakdown Structure o RBS), que describe las fuentes de riesgos en

proyectos utilizando una estructura jerárquica (Hillson, 2004). La RBS sirve como documentación de alto nivel para organizar la información de los riesgos, ordenando el proceso de gestión de riesgos en un documento estandarizado relevante en todos sus niveles (Plan Hammer, 2015). El objetivo de esta herramienta es definir los factores que dan origen a los riesgos y organizarlos en categorías, y cada una de las mismas, en sub-categorías o niveles. Una vez definido el RBS, este se puede utilizar para otros proyectos relacionados; sin embargo, no existe un modelo general que se adapte a todos los proyectos, por lo que se debe desarrollar un RBS personalizado según la industria, organización o tipo de proyecto (Sharma, s.f.). Se destaca que para la formulación de este modelo de gestión se deseó aplicarlo en una organización es particular para no formular un modelo teórico, sino uno aplicado y específico para un tipo de estructura organizacional. Por consiguiente, se diseñó un RBS específicamente para el esquema desarrollado para la Universidad de Río Negro y los riesgos de activos informáticos asociados. La Figura 2.1 detalla la estructura del mismo.

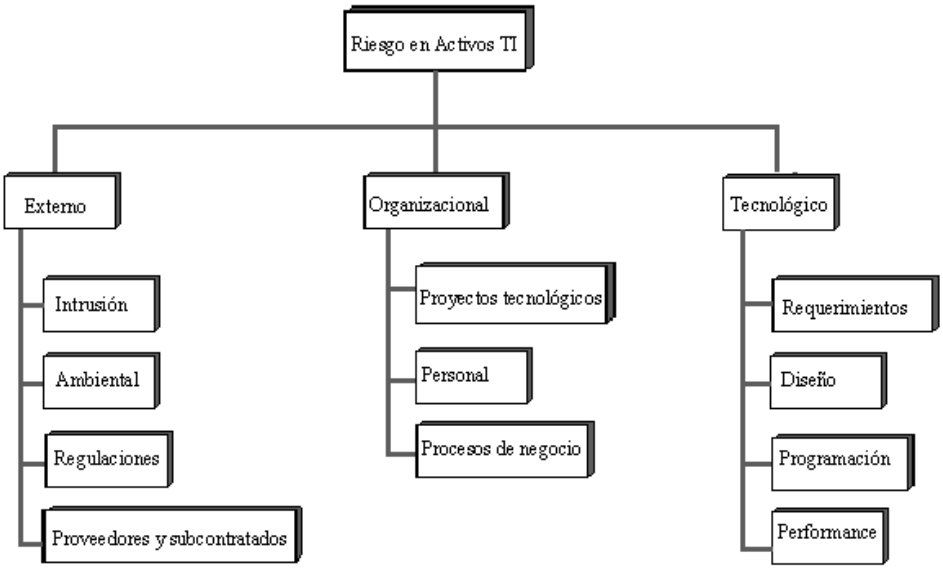

Figura 2.1. Estructura de Desglose de Riesgos en activos informáticos para la Universidad Nacional de Río Negro.

Es importante mencionar que esta clasificación reúne categorías más allá de las tecnológica, puesto que la definición de activos informáticos abarca todos los recursos de una organización que hacen uso de la información (Lugani y Peña, 2018), lo que también incluye a las personas, como proveedores y terceros. Con esta noción, se definieron tres grandes categorías de riesgos en el primer nivel del RBS:

1. Riesgo externo. Comprende aquellas amenazas causadas por factores externos al activo o a la organización, como accesos no autorizados, amenazas ambientales o regulaciones.
2. Riesgo organizacional. Incluye las situaciones de amenazas relacionadas con factores internos en la organización, como proyectos que involucren uso de tecnologías, así como el accionar del personal.
3. Riesgo tecnológico. También denominado como riesgo técnico, comprende las amenazas relacionadas con aspectos propios del activo informático (cuando el mismo es un recurso tecnológico), como son el análisis de requerimientos y el código fuente del programa.

En la sección siguiente se describen las categorías del segundo nivel de la jerarquía de riesgos propuesta.

2.1.1. Riesgos externos

- Intrusión. Contempla los riesgos relacionados con el acceso no autorizado de individuos o sistemas al activo informático, tanto el acceso físico como el remoto.
- Ambiental. Son aquellas situaciones donde los factores climáticos y de origen ambiental suponen un riesgo para el activo.
- Regulaciones. Implica los riesgos relacionados con el (in)cumplimiento de las normas y regulaciones vigentes que rigen el correcto funcionamiento del activo y la información utilizada por el mismo.
- Proveedores y subcontratados. Son aquellos riesgos relacionados con terceros y el cumplimiento de sus responsabilidades.

2.1.2. Riesgos organizacionales

- Proyectos tecnológicos. Involucra los riesgos existentes en aquellos proyectos tecnológicos o que incluyan alguna tecnología, en la especificación de responsabilidades en los contratos y el cumplimiento de las mismas.
- Personal. Abarca las amenazas asociadas al accionar del personal de la organización.
- Procesos de negocio. Involucra los riesgos que amenazan el flujo de los procesos de negocio donde se haga uso de, o participe, un activo informático.

2.1.3. Riesgos tecnológicos

- Requerimientos. Abarca aquellos riesgos relacionados con los requerimientos del sistema o recurso tecnológico.
- Diseño. Son los riesgos asociados al diseño del sistema o recurso tecnológico.
- Programación. Comprende los riesgos relacionados con el código fuente del sistema.
- Performance. Abarca los riesgos donde el activo se vea afectado por aspectos relacionados con su rendimiento o el de otros activos relacionados.

2.2. Definición de valores de probabilidad de ocurrencia e impacto del riesgo

La estandarización de los riesgos informáticos identificados (ej.: a través de un RBS) exige la asignación de valores probabilísticos para definir la ocurrencia del evento y su impacto en caso de concretarse tal amenaza, y así determinar su criticidad. Para la ocurrencia, la organización debe tener una noción clara acerca de la probabilidad de que suceda una amenaza, considerando todos los escenarios de riesgo posibles. La Tabla 2.1 considera los siguientes valores probabilísticos para la ocurrencia del riesgo.

Nivel de ocurrencia del riesgo	Valor probabilístico
Casi seguro que sucede	0.9
Muy probable que suceda	0.7
Posiblemente suceda	0.5
Difícil que suceda	0.3
Muy difícil que suceda	0.1

Tabla 2.1 Probabilidad de ocurrencia de los riesgos

Ha de mencionarse que no se tuvieron en cuenta los valores extremos, esto es, no existirá una probabilidad de ocurrencia de 0 o 1. Esto se debe a la naturaleza propia del riesgo, puesto que en caso de haber un evento con probabilidad de 1 (100%), entonces no es un riesgo sino una certeza de que tal eventualidad tendrá lugar. En este sentido si un evento ha ocurrido en el pasado, se tiene en cuenta que se han tomado las acciones de prevención adecuadas para bajar el riesgo de ocurrencia. Por lo tanto, no se tiene en cuenta un valor ocurrencia segura, o valores definidos por ocurrencias pasadas.

En el caso de una amenaza con una probabilidad nula (0%) no se considera como un riesgo y por consiguiente, no se tendrá en cuenta. Sin embargo, es muy difícil (cuando no imposible) tener la completa certeza de que una determinada eventualidad

no sucederá de ninguna manera, y con mayor razón en el ámbito de la seguridad de la información.

La definición del impacto del riesgo es un tanto más compleja que la ocurrencia del mismo, puesto que permite analizar el efecto potencial de la amenaza sobre diversos aspectos como el cronograma, el costo, la calidad y el desempeño (Project Management Institute, 2013). Continuando con el esquema definido por Lugani y Peña (2018), se determinó la evaluación del impacto del riesgo en términos de costo económico, de desempeño y de tiempo.

- Impacto sobre el tiempo: Tiene por objetivo determinar los efectos del riesgo sobre la cantidad de tiempo que un proceso significativo para la organización no estará disponible, produciendo retrasos, falta de disponibilidad en sistemas o transacciones, indisponibilidad de atención a usuarios u otras acciones que pueden ser tanto tangibles como las anteriores, como intangibles como ser una mala imagen de la institución ante falta de disponibilidad de un servicio. En la Tabla 2.2 se observan los valores asociados al impacto en términos de tiempo.

Impacto del riesgo sobre el tiempo	Valor equivalente
Retraso de varios días	0.9
Retraso de un día	0.7
Retraso de una hora	0.5
Retraso de hasta 15 minutos	0.3
No tiene un efecto considerable	0.1

Tabla 2.2 Impacto del riesgo sobre el tiempo

- Impacto sobre el desempeño: Busca definir la influencia de la amenaza sobre el funcionamiento del activo al que afecta, es decir, el porcentaje en que inhabilita las funciones del mismo. Esto se refleja en la Tabla 2.3.

Impacto del riesgo sobre el desempeño	**Valor equivalente**
Lo inhabilita en más del 75%	0.9
Lo inhabilita entre 50% y 75%	0.75
Lo inhabilita entre 10% y 50%	0.5
Lo inhabilita en menos de 10%	0.25

Tabla 2.3 Impacto del riesgo sobre el desempeño

- Impacto sobre la economía: Considera el efecto del riesgo sobre el activo en términos monetarios, si bien este sentido es amplio, la organización debe analizar

desde el reemplazo de activos hasta costos adicionales para que las operaciones se normalicen, incluso las erogaciones que se planifiquen realizar una vez restablecido el servicio, ya que todos estos costos deben tenerse en cuenta de ocurrir esta situación. En la Tabla 2.4 se observan los valores asociados a esta clase de impacto.

Impacto del riesgo sobre el costo	Valor equivalente
Tiene un costo muy elevado al del activo	0.9
Tiene un costo relativo similar al activo	0.5
Tiene un costo menor al del activo	0.3

Tabla 2.4 Impacto del riesgo sobre el costo económico

Las escalas o valores presentados en este esquema han sido sugeridos y diseñados para los fines prácticos de esta primera implementación del esquema de Riesgos, se concede que, en las sucesivas implementaciones del modelo en escenarios reales, los valores pueden sufrir modificaciones de acuerdo a la experiencia de los usuarios.

2.2.1. Matriz de probabilidad e impacto

Una vez que los riesgos son valorados cuantitativamente se deben presentar gráficamente y priorizarse para determinar aquellos que se gestionarán en primer lugar. Una herramienta útil para realizar esto es diseñar una matriz en donde se observe la probabilidad e impacto resultante de la asignación de valores de riesgo. Esta matriz permite demostrar a los administradores de este proceso los riesgos según su criticidad. Esta última viene dada por (como ya se mencionó anteriormente) la probabilidad de ocurrencia e impacto, por consiguiente, son estas dos variables las que constituyen los ejes de la matriz. Por lo anterior, es ésta una herramienta de análisis cualitativo de riesgos que nos permite priorizar los mismos (Muradas, 2016). Se definió a continuación la matriz de probabilidad e impacto que se utilizará durante la implementación el esquema de gestión de riesgo desarrollado anteriormente. La probabilidad ubicada en el eje vertical se encuentra definida por la siguiente escala: excepcional, improbable, probable, posible y cierto. El impacto, sobre el eje horizontal, tiene la escala: despreciable, marginal, moderado, crítico y catastrófico. Ambas escalas están definidas según Longares (2018). En la Tabla 2.5 se observa la clasificación del nivel de criticidad del riesgo según su valor. Esta criticidad viene dada en porcentajes.

Nivel de riesgo	Porcentaje de criticidad	Color asociado
Crítico	>40%	Rojo
Moderado	>10% y <40%	Amarillo
Mínimo	<10%	Verde

Tabla 2.5. Escala cualitativa de riesgos según su criticidad

A continuación, la Figura 2.6 detalla la matriz de probabilidad e impacto resultante de aplicar las escalas mencionadas, junto con el porcentaje de criticidad del riesgo.

Probabilidad/Impacto	Despreciable	Marginal	Moderado	Crítico	Catastrófico
Cierto	9%	27%	45%	63%	81%
Posible	7%	21%	35%	49%	63%
Probable	5%	15%	25%	35%	45%
Improbable	3%	9%	15%	21%	27%
Excepcional	1%	3%	5%	7%	9%

Figura 2.6. Matriz de probabilidad e impacto.

El objetivo del desarrollo de esta matriz es demostrar que para ciertos activos de información los riesgos identificados puedes ser críticos y por ello deben ser gestionados en lo inmediato. La agrupación de los riesgos en la matriz según sus valores es de gran valor para la organización ya que sustenta formalmente las acciones de prevención y protección que deben llevarse.

3. Diseño del monitoreo y evaluación de la gestión de riesgos

La definición de las herramientas descritas en la sección anterior complementa al esquema de gestión de riesgos en la UNRN ya definido. Sin embargo, la gestión de riesgos no concluye aquí, sino que debe continuar e través del seguimiento de los riesgos y la implementación de los planes de respuesta (PMO Informática, 2012). El monitoreo de la gestión de riesgos no sólo permite revisar y analizar la efectividad de lo planificado, sino que también favorece el cumplimiento de ciertos objetivos que describe Bollín (2000) y que a continuación se mencionan:

- Profesionalización del trabajo
- Aumento de la eficiencia y la eficacia del trabajo
- Ajuste continuo del trabajo a condiciones cambiantes
- Aprendizaje de éxitos y deficiencias
- Alineación continua del trabajo con los objetivos esperados.

Es por consiguiente una necesidad el realizar un seguimiento de las actividades previstas y analizar su cumplimiento, y para tal fin se definió un esquema de actividades para el monitoreo. La Figura 3.1 describe el marco de acción del esquema mencionado:

Etapa	Actividad/es	Entregable/s
1. Registro de ejecución de actividades planificadas	• Registrar el estado de realización de las acciones definidas de gestión de riesgo	• Informes de avance elaborados por los responsables definidos
2. Evaluación de desempeño del plan	• Analizar avances y variaciones en costo y/o tiempo según lo planificado y sus causas • Revisar indicadores actuales de desempeño y comparar con KPIs definidos • Verificar el grado de efectividad de controles y planes de respuesta implementados	• Avances y variaciones de acción planificada en función de costo y tiempo • Evaluación de las acciones de seguridad implementadas
3. Seguimiento de riesgos tratados	• Verificar estado actual de los riesgos tratados • Analizar riesgos residuales • Verificar la ocurrencia de amenazas durante la implementación • Verificar estado de riesgos no evadidos, mitigados o transferidos • Identificar posibles nuevos riesgos	• Informe de estado de riesgos tratados, no tratados y residuales • Documento con posibles nuevos riesgos para analizar
4. Evaluación de auditorías	• Evaluar cumplimiento de las actividades de auditoría planificadas • Evaluar los resultados de auditoría en función de lo analizado anteriormente	• Informe de auditoria
5. Toma de decisiones para ajustes necesarios.	• Definir cambios en los cronogramas, actividades, etc. • Analizar modificaciones de planes de respuesta a los riesgos	• Calendario de cambios

	• Definir riesgos a excluir en la gestión de los mismos	
6. Comunicación de resultados de monitoreo	• Comunicar acerca de lo realizado en las etapas precedentes	• Informe final de monitoreo y evaluación

Figura 3.1. Esquema de monitoreo y evaluación de gestión de riesgos.

Finalmente, la aplicación de las actividades descritas en este esquema resultará en la información necesaria para desarrollar la siguiente iteración y así retroalimentar al proceso de gestión de riesgos, otorgando una mejora continua del mismo.

4 Conclusiones

El esquema de cuatro fases planteado por Lugani y Peña (2018) para la gestión de riesgos en la UNRN requería de herramientas que permitan su implementación en la organización, así como un seguimiento a fin de evaluar el desempeño del proceso y mejorarlo. Por ello, se elaboró una Estructura de Desglose del Riesgo (RBS) con el objetivo de clasificar los riesgos en diferentes categorías, y se diseñaron tablas de valores para el análisis cuantitativo de los riesgos identificados, en función de su probabilidad e impacto. A partir de esos valores se armó un modelo de matriz de probabilidad e impacto que permita agrupar los riesgos según su criticidad y así permitir a la organización el tratamiento de aquellos más significativos en primer lugar. Se destaca que también esta matriz es útil para priorizar tareas ya que frecuentemente los recursos disponibles por las organizaciones son limitados y por lo tanto se debe seleccionar muy cuidadosamente donde ubicar los recursos con que se cuenta.

Asimismo, el esquema de actividades destinadas al desarrollo del monitoreo y evaluación de la gestión de riesgos favorecerá la mejora continua del proceso. Con el presente artículo se da conclusión a la definición del esquema de gestión de riesgos informáticos, que ha sido diseñado para la gestión de activos informáticos de la Universidad Nacional de Río Negro. Este proceso se mejorará continuamente, a fin de estar permanentemente alineado a las mejores prácticas de seguridad de la información, manteniendo la organización protegida o preparada ante cualquier eventualidad que pueda suceder y apostar así a la generación continua de valor.

Referencias

1. Bollin, C. (2000). Planificación, Monitoreo y Evaluación para un Sistema de Gestión Local de Riesgo. Proyecto para el Fortalecimiento de Estructuras Locales en la Mitigación de Desastres (FEMID). Guatemala. Recuperado de

http://saludpublica.bvsp.org.bo/textocompleto/bvsp/boxp68/gestion_de_riesgo.pdf [Consultado 05 Abr., 2019]
2. Halling, G. (08 de Mayo de 2015). The importance of a Risk Breakdown Structure (RBS). General Interest Asset Managers Consultants Contractors, Risk Tools. Recuperado de https://www.risktools.com.au/blog/risk-identification-management-RBS/ [Consultado 03 Abr., 2019]
3. Hillson, D. (2004). Describiendo el Riesgo:¿Cuántos Detalles?(p.1). Risk Doctor. Recuperado de http://www.risk-doctor.com/pdf-briefings/risk-doctor09s.pdf [Consultado 01 Abr., 2019]
4. Hoogenraad, W. (10 de Noviembre de 2018). La utilidad de una Estructura de Desglose de Riesgos (RBS). ITPedia. Recuperado de https://www.itpedia.nl/es/2017/05/17/het-nut-van-een-risico-breakdown-structure-rbs/ [Consultado 15 Mar., 2019]
5. Longares, O. (2018). Matriz Probabilidad-Impacto: Analizando los riesgos de forma visual. Activa Conocimiento. Recuperado de http://activaconocimiento.es/matriz-probabilidad-impacto/ [Consultado 17 Mar., 2019]
6. Lugani, C.F. y Peña, R.L. (2018). Desarrollo de un esquema de Gestión de Riesgos para la Universidad Nacional de Río Negro. Anales de SIE 2018, Simposio de Informática en el Estado, 47º Jornadas Argentinas de Informática e Investigación Operativa (JAIIO), 170-182. ISSN: 2451-7534. Recuperado de http://47jaiio.sadio.org.ar/sites/default/files/SIE-14.PDF [Consultado 10 Mar., 2019]
7. Mendoza, M.A. (30 de Septiembre de 2014). 8 pasos para hacer una evaluación de riesgos (parte II). We live security. Recuperado de https://www.welivesecurity.com/la-es/2014/09/30/8-pasos-evaluacion-de-riesgos-2/ [Consultado 10 Mar., 2019]
8. Muradas, S. (03 de Febrero de 2016). La matriz Probabilidad-Impacto. Recuperado de https://www.eoi.es/blogs/mcalidadon/2016/02/03/la-matriz-probabilidad-impacto/ [Consultado 15 Mar., 2019]
9. Pérez, A. (8 de Noviembre de 2016). Cómo crear una Efectiva Matriz de Riesgos en tan sólo 3 Pasos. CEO Level. Recuperado de http://www.ceolevel.com/como-crear-una-efectiva-matriz-de-riesgos-en-tan-solo-3-pasos [Consultado 02 Abr., 2019]
10. Plan Hammer. (14 de Diciembre de 2015). Why You Should Use Risk Registers or a Risk Breakdown Structure on Your Project?. Plan Hammer Blog. Recuperado de https://planhammer.io/blog/risk-register-tool/why-you-should-use-a-risk-register-or-risk-breakdown-structure-on-your-project/ [Consultado 01 Abr., 2019]
11. PMO Informática. (15 de Octubre de 2012). Cómo hacer el seguimiento de los riesgos en proyectos. PMO Informática. Recuperado de http://www.pmoinformatica.com/2012/10/pasos-seguimiento-riesgos-proyecto.html [Consultado 27 Mar., 2019]
12. Project Management Institute. (2013). Capítulo 11: Gestión de los riesgos del proyecto. En Project Management Institute. (Ed.). Guía del PMBOK, 5ta Edición. Pensilvania, Estados Unidos: Project Management Institute.
13. Sharma, R. (s.f.). Organizing Risks With a Risk Breakdown Structure (RBS). Bright Hub Project Management. Recuperado de https://www.brighthubpm.com/risk-management/51997-using-a-risk-breakdown-structure/ [Consultado 03 Abr., 2019]